Counting points on (more general) curves

Jan Tuitman, KU Leuven

November 14, 2013

Zeta functions

Suppose that

- $\mathbf{F}_q$ finite field of cardinality $q = p^n$.
- $X/\mathbf{F}_q$ a smooth proper algebraic curve of genus g.

Recall that the zeta function of X is defined as

$$Z(X, T) = \exp\left(\sum_{i=1}^{\infty} |X(\mathbf{F}_{q^i})| \frac{T^i}{i}\right).$$

It follows from the Weil conjectures that $Z(X, T)$ is of the form

$$\frac{\chi(T)}{(1-T)(1-qT)},$$

where $\chi(T) \in \mathbf{Z}[T]$ of degree $2g$, with inverse roots that

- have absolute value $q^{\frac{1}{2}}$
- are permuted by the map $x \to q/x$.

Computing zeta functions

Problem

How to compute $Z(X, T)$ (efficiently)?

Note that this problem has cryptographic applications when X is a (hyper)elliptic curve.

Theorem

Let F_p denote the pth power Frobenius map and $H^*_{rig}(X)$ the rigid cohomology. Then

$$\chi(T) = \det(1 - T\,\mathrm{F}_p^n \,|\, H^1_{rig}(X)).$$

Hyperelliptic curves

Suppose that $p \neq 2$. A hyperelliptic curve X is given by an (affine) equation of the form

$$y^2 = Q(x),$$

with $Q \in \mathbf{F}_q[x]$ a monic polynomial of degree $2g+1$ with $\gcd(Q, Q') = 1$.

To define $H^1_{\mathrm{rig}}(X)$, we start by lifting Q to characteristic 0:

Let $\mathcal{Q} \in \mathbf{Z}_q[x]$ denote a monic lift of Q of degree $2g+1$.

Some rings

We define a ring $\mathbf{Z}_q\langle x, y, y^{-1}\rangle^\dagger$ of overconvergent functions:

$$\{\sum_{i=0}^{\infty}\sum_{j=-\infty}^{\infty} a_{i,j}x^i y^j | a_{i,j} \in \mathbf{Z}_q, \exists \rho > 1 \colon \lim_{i+|j|\to\infty} |a_{i,j}|\rho^i = 0\}.$$

Moreover, we denote

$$\mathcal{R} = \mathbf{Z}_q[x, y, y^{-1}]/(\mathcal{Q}), \quad \mathcal{R}^\dagger = \mathbf{Z}_q\langle x, y, y^{-1}\rangle^\dagger/(\mathcal{Q})$$

$$\mathcal{U} = \operatorname{Spec}\mathcal{R}, \qquad \mathbb{U} = \mathcal{U} \otimes \mathbf{Q}_q, \qquad U = \mathcal{U} \otimes \mathbf{F}_q.$$

Rigid cohomology

We define the overconvergent Kähler differentials

$$\Omega^1_{\mathcal{R}^\dagger} = \frac{R^\dagger dx \oplus R^\dagger dy}{(2ydy - Q' dx)}$$

and the overconvergent De Rham complex

$$\Omega^\bullet_{\mathcal{R}^\dagger} : \quad 0 \longrightarrow \mathcal{R}^\dagger \xrightarrow{d} \Omega_{\mathcal{R}^\dagger} \longrightarrow 0.$$

We then have

$$H^1_{\mathrm{rig}}(U) = H^1(\Omega^\bullet_{\mathcal{R}^\dagger} \otimes \mathbf{Q}_q) = \mathrm{coker}(d) \otimes \mathbf{Q}_q.$$

Frobenius lift

The pth power Frobenius map on $\mathcal{R} \otimes \mathbf{F}_q$ can be lifted to $\mathcal{R}$.

If $\sigma \in \mathrm{Gal}(\mathbf{Q}_q/\mathbf{Q}_p)$ denotes the unique lift of the pth power Frobenius map on $\mathbf{F}_q$, then

$$F_p(y)^2 = \mathcal{Q}^\sigma(F_p(x)).$$

So we define

$$F_p(x) = x^p,$$
$$F_p(y) = \mathcal{Q}^\sigma(x^p)^{\frac{1}{2}} = y^p \left(1 + \frac{\mathcal{Q}^\sigma(x^p) - \mathcal{Q}(x)^p}{y^{2p}}\right)^{\frac{1}{2}}.$$

The square root can be computed efficiently by Hensel lifting.

Computing in the cohomology

We can write any 1-form $\omega \in \Omega_{\mathcal{R}^\dagger}$ as

$$\sum_{i=-\infty}^{\infty} \frac{a_i(x)}{y^i} dx,$$

with $a_i \in \mathbf{Z}_q[x]$ of degree $< 2g+1$ for all $i \in \mathbf{Z}$. Writing $B(x) = A_1(x)\mathcal{Q}(x) + A_2(x)Q'(x)$, we have

$$B(x)\frac{dx}{y^i} \equiv \left(A_1(x) + \frac{2A_2'(x)}{(i-2)}\right)\frac{dx}{y^{i-2}}.$$

This allows us to eliminate all terms with $i > 2$. We can do something similar for the terms with $i \leq 0$.

A basis for the cohomology

As a consequence, one can show that:

Theorem

A basis for $H^1_{rig}(U)$ is given by

$$[x^0 \frac{dx}{y}, \ldots, x^{2g-1}\frac{dx}{y}, x^0\frac{dx}{y^2}, \ldots, x^{2g}\frac{dx}{y^2}]$$

and the first $2g$ vectors form a basis for the subspace $H^1_{rig}(X)$.

Kedlaya's algorithm

A rough sketch:

- Compute $F_p(\frac{1}{y})$ and $F_p(x^i \frac{dx}{y}) = px^{ip+p-1} F_p(\frac{1}{y}) dx$.
- Reduce back to the basis $[x^0 \frac{dx}{y}, \ldots, x^{2g-1} \frac{dx}{y}]$ and read off the matrix A of F_p on $H^1_{\mathrm{rig}}(X)$.
- Compute the matrix $A^{(n)} = A^{\sigma^{n-1}} \ldots A^{\sigma} A$ of F_p^n on $H^1_{\mathrm{rig}}(X)$.
- Determine $\chi(T) = \det(1 - \mathrm{F}_p^n T | H^1_{\mathrm{rig}}(X))$.

The polynomial $\chi(T) = \sum_{i=0}^{2g} \chi_i T^i \in \mathbf{Z}[T]$ is determined exactly if known to high enough p-adic precision, since there are explicit bounds for the size of its coefficients.

More general curves

We let $X/\mathbf{F}_q$ denote the smooth projective curve given by the (affine) equation

$$Q(x,y) = y^d + Q_{d-1}(x)y^{d-1} + \ldots + Q_0 = 0,$$

where $Q(x,y)$ is irreducible separable and $Q_i(x) \in \mathbf{F}_q[x]$ for all $0 \leq i \leq d-1$.

We let $\mathcal{Q} \in \mathbf{Z}_q[x]$ denote a lift of Q that is monic of degree d in y.

Proposition

The $\mathbf{Z}_q[x]$-module $\mathbf{Z}_q[x,y]/(\mathcal{Q})$ is free with basis $[1, y, \ldots, y^{d-1}]$.

Some notation

Definition

We let $\Delta(x) \in \mathbf{Z}_q[x]$ *denote the resultant of* $\mathcal{Q}$ *and* $\frac{\partial \mathcal{Q}}{\partial y}$ *with respect to the variable* y *and* $r(x) \in \mathbf{Z}_q[x]$ *the squarefree polynomial* $r = \Delta/(\gcd(\Delta, \frac{d\Delta}{dx}))$.

Note that $\Delta(x) \neq 0 \pmod{p}$ since the map x is separable.

Definition

$$\mathcal{S} = \mathbf{Z}_q[x, \frac{1}{r}], \qquad \mathcal{R} = \mathbf{Z}_q[x, \frac{1}{r}, y]/(\mathcal{Q}),$$
$$\mathcal{S}^\dagger = \mathbf{Z}_q\langle x, \frac{1}{r}\rangle^\dagger, \qquad \mathcal{R}^\dagger = \mathbf{Z}_q\langle x, \frac{1}{r}, y\rangle^\dagger/(\mathcal{Q}),$$

and write $\mathcal{V} = \operatorname{Spec}\mathcal{S}$, $\mathcal{U} = \operatorname{Spec}\mathcal{R}$, *so that* x *defines a finite étale morphism from* $\mathcal{U}$ *to* $\mathcal{V}$.

The following assumption is essential:

Assumption

1. *There exists a smooth proper curve* $\mathcal{X}$ *over* $\mathbf{Z}_q$ *and a smooth relative divisor* $\mathcal{D}_{\mathcal{X}}$ *on* $\mathcal{X}$ *such that* $\mathcal{U} = \mathcal{X} \setminus \mathcal{D}_{\mathcal{X}}$. *We write* $\mathbb{X} = \mathcal{X} \otimes \mathbf{Q}_q$ *for the generic fibre of* $\mathcal{X}$.
2. *There exists a smooth relative divisor* $\mathcal{D}_{\mathbf{P}^1}$ *on* $\mathbf{P}^1_{\mathbf{Z}_q}$ *such that* $\mathcal{V} = \mathbf{P}^1_{\mathbf{Z}_q} \setminus \mathcal{D}_{\mathbf{P}^1}$.

Definition

We let $U = \mathcal{U} \otimes_{\mathbf{Z}_q} \mathbf{F}_q$, $V = \mathcal{V} \otimes_{\mathbf{Z}_q} \mathbf{F}_q$ *denote the special fibres and* $\mathbb{U} = \mathcal{U} \otimes_{\mathbf{Z}_q} \mathbf{Q}_q$, $\mathbb{V} = \mathcal{V} \otimes_{\mathbf{Z}_q} \mathbf{Q}_q$ *the generic fibres of* $\mathcal{U}$ *and* $\mathcal{V}$, *respectively.*

For convenience, we assume:

Assumption

The zero locus of $\mathcal{Q}$ in $\mathbf{A}^2_{\mathbf{Z}_q}$ is smooth over $\mathbf{Z}_q$.

Proposition

The element $s = r/\frac{\partial \mathcal{Q}}{\partial y}$ of $\mathbf{Q}_q(x, y)$ is contained in $\mathbf{Z}_q[x, y]/(\mathcal{Q})$.

Sketch of the proof: $\Delta/\frac{\partial \mathcal{Q}}{\partial y}$ is contained in $\mathbf{Z}_q[x, y]/(\mathcal{Q})$ by the definition of Δ as the determinant of the Sylvester matrix. By the assumption, $[1, y, \ldots, y^{d-1}]$ is an integral basis of $\mathbf{Q}_q[x, y]/(\mathcal{Q})$ over $\mathbf{Q}_q[x]$. So for any monic irreducible polynomial $\pi \in \mathbf{Z}_q[x]$, the element $\frac{\partial \mathcal{Q}}{\partial y}/\pi$ of $\mathbf{Q}_q(x, y)$ is not integral at (π) because of the term $(d/\pi)y^{d-1}$, hence its inverse $\pi/\frac{\partial \mathcal{Q}}{\partial y}$ is integral (even zero) at (π). Since $\prod_{\pi|\Delta} \pi = r$, this proves the Proposition.

Frobenius lift

Define sequences $(\alpha_i)_{i\geq 0}$, $(\beta_i)_{i\geq 0}$, with $\alpha_i \in S^\dagger$ and $\beta_i \in \mathcal{R}^\dagger$, by the following recursion:

$$\begin{aligned}
\alpha_0 &= \frac{1}{r^p}, \\
\beta_0 &= y^p, \\
\alpha_{i+1} &= \alpha_i(2 - \alpha_i r^\sigma(x^p)) && \pmod{p^{2^{i+1}}}, \\
\beta_{i+1} &= \beta_i - \mathcal{Q}^\sigma(x^p, \beta_i) s^\sigma(x^p, \beta_i)\alpha_i && \pmod{p^{2^{i+1}}}.
\end{aligned}$$

Then one easily checks that the σ-semilinear ringhomomorphism $\mathrm{F}_p : \mathcal{R}^\dagger \to \mathcal{R}^\dagger$ defined by

$$\mathrm{F}_p(x) = x^p, \qquad \mathrm{F}_p(\frac{1}{r}) = \lim_{i\to\infty} \alpha_i, \qquad \mathrm{F}_p(y) = \lim_{i\to\infty} \beta_i,$$

is a Frobenius lift.

The connection matrix

Definition

Let $M \in M_{d\times d}(\mathbf{Z}_q[x])$ *denote the matrix for which*

$$d(y^j) = jy^{j-1}dy = -jy^{j-1}\frac{s}{r}\frac{\partial \mathcal{Q}}{\partial x}dx = \sum_{i=0}^{d-1}\left(\frac{M_{ij}}{r}\right)y^i dx,$$

for all $0 \leq j \leq d-1$ *as* 1*-forms on* $\mathcal{U}$.

For convenience, we assume:

Assumption

$\deg(M) < \deg(r)$, *or equivalently* $(M/r)dx$ *has at most a simple pole at* $x = \infty$.

The exponents

Definition

Let $x_0 \in \mathbf{P}^1(\bar{\mathbf{Q}}_q)$ be a geometric point $\neq \infty$. The exponents of $(M/r)dx$ at x_0 are defined as the eigenvalues of the residue matrix $(x - x_0)(M/r)|_{x=x_0}$. Moreover, the exponents of $(M/r)dx$ at ∞ are defined as its exponents at $t = 0$, after substituting $x = 1/t$.

Proposition

The exponents of $(M/r)dx$ at any point $x_0 \in \mathbf{P}^1(\bar{\mathbf{Q}}_q)$ are elements of $\mathbf{Q} \cap \mathbf{Z}_p$. For $x_0 \neq \infty$ they are contained in the interval $[0, 1)$ and for $x_0 = \infty$ in the interval $[(d-1)\mu, 0]$, where

$$\mu = \min\{\frac{\mathrm{ord}_P(y)}{e_P} : P \in x^{-1}(\infty)\}.$$

Effective convergence bounds

Proposition

Let $N \in \mathbf{N}$. Then modulo p^N:

1. $\mathrm{F}_p(1/r)$ *is congruent to* $\sum_{i=p}^{pN} \frac{\rho_i(x)}{r^i}$, *where for all* $p \leq i \leq pN$ *the polynomial* $\rho_i \in \mathbf{Z}_q[x]$ *satisfies* $\deg(\rho_i) < \deg(r)$.
2. $\mathrm{F}_p(y^i)$ *is congruent to* $\sum_{j=0}^{d-1} \phi_{i,j}(x) y^j$, *where*

$$\phi_{i,j} = \sum_{k=0}^{p(N-1)+1} \frac{\phi_{i,j,k}(x)}{r^k},$$

for all $0 \leq i,j \leq d-1$ *and* $\phi_{i,j,k} \in \mathbf{Z}_q[x]$ *satisfies* $\deg(\phi_{i,j,0}) < p(d-1)(-\mu)$ *and* $\deg(\phi_{i,j,k}) < \deg(r)$, *for all* $0 \leq i,j \leq d-1$ *and* $1 \leq k \leq p(N-1)+1$.

Sketch of the proof: Effective bounds for Frobenius structures on connections, T. and Kedlaya, 2013.

Computing in the cohomology I

Proposition

For all $\ell \in \mathbf{N}$ and every vector $w \in \mathbf{Q}_q[x]^{\oplus d}$, there exist (unique) vectors $u, v \in \mathbf{Q}_q[x]^{\oplus d}$ with $\deg(v) < \deg(r)$, such that

$$\frac{\sum_{i=0}^{d-1} w_i y^i}{r^\ell} \frac{dx}{r} = d\left(\frac{\sum_{i=0}^{d-1} v_i y^i}{r^\ell}\right) + \frac{\sum_{i=0}^{d-1} u_i y^i}{r^{\ell-1}} \frac{dx}{r}$$

as 1-forms on $\mathbb{U}$.

Sketch of the proof: r is separable, so r' is invertible in $\mathbf{Q}_q[x]/(r)$. v has to satisfy $\left(\frac{M}{r'} - \ell I\right) v \equiv \frac{u}{r'} \pmod{r}$ over $\mathbf{Q}_q[x]/(r)$. The finite exponents of $(M/r)dx$ are contained in $[0, 1)$, hence $\det(\ell I - M/r')$ is invertible in $\mathbf{Q}_q[x]/(r)$, so there is a unique solution v. We now take

$$u = \frac{w - \left(M - \ell r' I\right) v}{r} - \frac{dv}{dx}.$$

Computing in the cohomology II

Proposition

For every vector $w \in \mathbf{Q}_q[x]^{\oplus d}$ with $\deg(w) \geq \deg(r)$, there exist vectors $u, v \in \mathbf{Q}_q[x]^{\oplus d}$ with $\deg(u) < \deg(w)$, such that

$$(\sum_{i=0}^{d-1} w_i y^i)\frac{dx}{r} = d(\sum_{i=0}^{d-1} v_i y^i) + (\sum_{i=0}^{d-1} u_i y^i)\frac{dx}{r}$$

as 1-forms on $\mathbb{U}$.

Sketch of the proof: We denote $t = 1/x$. Since $\deg(M) < \deg(r)$, we can expand $\frac{M}{r}dx = \left(\frac{M_{-1}}{t} + M_0 + \ldots\right)dt$, where $M_i \in M_{d\times d}(\mathbf{Q}_q)$ for all i. Similarly, if $k = \deg(w) - \deg(r) + 2$, then we can write $(\sum_{i=0}^{d-1} w_i y^i)\frac{dx}{r} = \left(\frac{b_{-k}}{t^k} + \frac{b_{-(k-1)}}{t^{k-1}} + \ldots\right)dt$, where $b_i \in (\mathbf{Q}_q)^{\oplus d}$ for all i. The infinite exponents of $(M/r)dx$ are ≤ 0, so the linear system $(M_{-1} - (k-1)I)c = b_{-k}$ has a unique solution $c \in (\mathbf{Q}_q)^{\oplus d}$. We now take

$$v = cx^{k-1} \text{ and } u = w - (Mv + r\tfrac{dv}{dx}).$$

Theorem

Every class in $H^1_{rig}(U)$ *is represented by a* 1*-form of the form*

$$(\sum_{i=0}^{d-1} u_i(x)y^i)\frac{dx}{r},$$

where $u_i \in \mathbf{Q}_q[x]$ *satisfies* $\deg(u_i) < \deg(r)$ *for all* $0 \leq i \leq d-1$*.*

Sketch of the proof: By a comparison theorem of Baldassarri and Chiarellotto, we can restrict to classes that lie in $H^1_{\mathrm{dR}}(\mathbb{U})$. Using the previous two propositions (both repeatedly), such a class can be reduced to the required form.

Precision loss I

Proposition

Let $\omega \in \Omega^1_{\mathcal{U}}$ *be of the form*

$$\omega = \frac{\sum_{i=0}^{d-1} w_i(x) y^i}{r^\ell} \frac{dx}{r},$$

where $\ell \in \mathbf{N}$ *and* $w_i \in \mathbf{Z}_q[x]$ *satisfies* $\deg(w_i) < \deg(r)$ *for all* $0 \leq i \leq d-1$. *We define* $e_0 = \max\{e_P | P \in \mathcal{X} \setminus \mathcal{U}, x(P) \neq \infty\}$. *If we represent the class of* ω *in* $H^1_{rig}(U)$ *as in the Theorem using the Proposition, then*

$$p^{\lfloor \log_p(\ell e_0) \rfloor} u_i(x) \in \mathbf{Z}_q[x]$$

for all $0 \leq i \leq d-1$.

Precision loss II

Proposition

Let $\omega \in \Omega^1_{\mathcal{U}}$ *be of the form*

$$\omega = (\sum_{i=0}^{d-1} w_i(x)y^i)\frac{dx}{r},$$

where $w_i \in \mathbf{Z}_q[x]$ *for all* $0 \leq i \leq d-1$ *and* $\deg(w_i) \geq \deg(r)$ *for some* $0 \leq i \leq d-1$. *We define* $m = (\deg(w) - \deg(r) + 1)$ *and* $e_\infty = \max\{e_P | P \in \mathcal{X} \setminus \mathcal{U}, x(P) = \infty\}$. *If we represent the class of* ω *in* $H^1_{rig}(U)$ *as in the Theorem using the Proposition, then*

$$p^{\lfloor \log_p((m-(d-1)\mu)e_\infty) \rfloor} u_i(x) \in \mathbf{Z}_q[x]$$

for all $0 \leq i \leq d-1$.

A basis for the cohomology

First, let E denote the $\mathbf{Q}_q$-vector space of 1-forms

$$\omega = (\sum_{i=0}^{d-1} u_i(x) y^i) \frac{dx}{r},$$

where $u_i \in \mathbf{Q}_q[x]$ satisfies $\deg(u_i) < \deg(r)$ for all $0 \leq i \leq d-1$. Now, let E_1 denote the kernel of the map that sends $\omega \in E$ to the element $\frac{\partial Q}{\partial y} \sum_{i=0}^{d-1} u_i y^i$ of $\mathbf{Q}_q[x,y]/(\mathcal{Q}, r)$. Finally, let E_2 denote the subspace of E_1 generated by the elements $d(y^i)$ for all $0 \leq i \leq d-1$.

Theorem

We have isomorphisms:

$$H^1_{rig}(U) \cong E/E_2, \qquad H^1_{rig}(X - x^{-1}(\infty)) \cong E_1/E_2.$$

Some remarks

- This allows us to compute $Z(X - x^{-1}(\infty), T)$, from which $Z(X, T)$ can be easily obtained.
- All assumptions but the first one can be removed by temporarily changing from $[y^0, \cdots, y^{d-1}]$ to another basis if equations for $\mathcal{X}$ are known.
- The way we compute in the cohomology is inspired by work of Lauder (and his student Walker) on the so called fibration method.

An example

Hyperelliptic curve $y^2 = f(x)$ with f of degree $2g + 1$.

$\Delta(x) = r(x) = f(x)$.

$$(M/r)dx = \begin{pmatrix} 0 & 0 \\ 0 & \frac{f'(x)}{2f(x)} \end{pmatrix} \mathrm{dx}$$

Finite exponents $0, 1/2$ and infinite ones $-(2g + 1)/2, 0$.

$$\begin{aligned} E &= \{(u_0(x) + u_1(x)y)dx/y^2\} \\ E_1 &= \{u_1(x)ydx/y^2\} \\ E_2 &= \{f'(x)ydx/y^2\} \end{aligned}$$

This gives the same basis for the cohomology as before.